

**\* NOTICES \***

JPO and NCIP are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**CLAIMS**

---

[Claim(s)]

[Claim 1] It is a computer system using the mouse with an identification function by the fingerprint which is the computer system which comes to have an indicator, an operation control machine, and the keyboard and the mouse as external input equipment at least, and is characterized by for said mouse to form a means move the cursor on said indicator, and a fingerprint detection means detect a fingerprint to said mouse while having the function perform informational selection and cancellation / activation directions, in said mouse.

[Claim 2] Said fingerprint detection means is a computer system using the mouse with an identification function by the fingerprint according to claim 1 characterized by consisting of a CCD sensor as an image pick-up means to picturize the light from the light source as a Mitsuteru gunner stage, the prism as a reflective means of light which reflects the light from said light source, and said prism.

[Claim 3] Said fingerprint detection means is a computer system using the mouse with an identification function by the fingerprint according to claim 1 characterized by becoming by the semi-conductor sensor.

[Claim 4] A registration means to register the fingerprint information as which said operation control machine was inputted from said fingerprint detection means, A collating means to collate the fingerprint information read from said fingerprint detection means for every fixed time amount, and registered fingerprint information, The computer system using the mouse with an identification function by the fingerprint according to claim 1 characterized by coming to have the management tool of the fingerprint which makes a judgment of authorization of access to said computer system, or disapproval by the collating result of said collating means.

[Claim 5] It is the identification approach using the computer system which comes to have an indicator, an operation control machine, and the keyboard and mouse as external input equipment at least. Said mouse The identification approach in the computer system characterized by detecting the fingerprint which performs a discernment judging of an individual with a fingerprint detection means to detect a means to move the cursor on said drop, and the fingerprint which came to have the function to perform informational selection and cancellation / activation directions, and was formed in said mouse.

---

[Translation done.]

**\* NOTICES \***

JPO and NCIP are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention aims at improvement in the security function about discernment of the individual by the mouse equipped with the fingerprint detection means, and relates to the identification approach in the computer system and this computer system using the mouse with an identification function by the fingerprint which can moreover perform discernment management of the individual by said mouse automatically into the operating status of a computer system.

[0002]

[Description of the Prior Art] In recent years, as for the computer system, the activity of a password is achieved with the spread of the Internet, the networks in an enterprise, etc. for two or more users' specification. When a password is in agreement, authorization or the disapproval of the activity of a computer system, access to a database, etc. is planned by connection with the Internet, connection with a network, and the list.

[0003] While there is convenience that specification of a user can perform utilization of such a password easily, since it is sufficient if it puts in once, if a computer system is working, even if said password will be a third party who does not know said password, it can access the interior of said system easily. Moreover, it has been the technical problem which should be improved also when becoming possible to carry out unjust utilization of said computer system simply from a power up and aiming at improvement in the security function of a computer system, if said password is known by others and used unjustly.

[0004] Registering not a password but the fingerprint for every individual of a user, judging authorization or the disapproval of access to a computer system as a means to aim at the improvement of such security, after preparing separately the fingerprint reading dedicated device which is another equipment at the time of the activity of a computer system and taking the necessary procedure for fingerprint authentication, and securing improvement in the security function of a computer system is performed.

[0005]

[Problem(s) to be Solved by the Invention] Since a check of a user with the password mentioned above is what usually consists of a figure, combination of an alphabetic character and a notation, etc., There is a problem that access will become possible freely until it changes a password once it is comparatively easy to decode and will decode. Moreover, the fingerprint reader which is a dedicated device for reading the fingerprint of said computer system although a check of the user by collating of a fingerprint improves from the field of security, since fingerprints differ for every individual is needed separately. The technical problem that space-saving-ization will become difficult in today when downsizing is being achieved, and it will moreover become expensive occurs. And whenever this fingerprint reader collates a fingerprint, a fingerprint authentication procedure is needed separately and it lacks in convenience. Moreover, it has been the technical problem which there is a possibility that it may not check even if a user replaces on the way, since utilization of a computer system can be performed without [ once it passes said fingerprint reader to collating in a fingerprint authentication procedure / henceforth ] collating of a fingerprint, but it may be used unjustly, and should be improved on the security of a computer system.

[0006] Then, this invention is accomplished in view of said Prior art, and improvement in the security function of a computer system is aimed at using the fingerprint established as identification of an individual, i.e., individual distinction, or the discernment approach. Namely, the image of a fingerprint reads in the fingerprint detection means of said mouse for every fixed time amount, collating with this read fingerprint data and the registered fingerprint data performs, and it aims at offering the identification approach in the computer system and this computer system using the mouse with an identification function by the fingerprint which can identify a user by forming a fingerprint detection means in the mouse which is external input equipment.

[0007] Moreover, by having formed the fingerprint detection means in the mouse, a user does not need to perform a fingerprint authentication procedure separately with the fingerprint reader as a dedicated device, and it aims at offering the identification approach in the computer system and this computer system using the mouse with an identification function by the fingerprint excellent in convenience.

[0008] Moreover, also in domestic, it excels in security by the rapid spread of the Internet, moreover a thing of a cheap configuration is desired, and it aims at offering the identification approach in the computer system and this computer system using the mouse with an identification function by the suitable fingerprint also seen from this field in recent years.

[0009]

[Means for Solving the Problem] The computer system using the mouse with an identification function by the fingerprint by this invention is a computer system which comes to have an indicator, an operation control machine, and the keyboard and the mouse as external input equipment at least, and said mouse forms a means move the cursor on said indicator, and a fingerprint detection means detect a fingerprint to said mouse while having the function perform informational selection and cancellation / activation directions in said mouse.

[0010] Moreover, said fingerprint detection means of the computer system using the mouse with an identification function by the fingerprint by this invention consists of a CCD sensor as an image pick-up means to picturize the light from the light source as a Mitsuteru gunner stage, the prism as a reflective means of light which reflects the light from said light source, and said prism.

[0011] Moreover, said fingerprint detection means of the computer system using the mouse with an identification function by the fingerprint by this invention becomes by the semi-conductor sensor.

[0012] Moreover, said operation control machine of the computer system using the mouse with an identification function by the fingerprint by this invention A collating means to collate a registration means to register the fingerprint information inputted from said fingerprint detection means, and the fingerprint information read from said fingerprint detection means for every fixed time amount and registered fingerprint information, It comes to have the management tool of the fingerprint which makes a judgment of authorization of access to said computer system, or disapproval by the collating result of said collating means.

[0013] Moreover, the identification approach in the computer system by this invention It is the identification approach using the computer system which comes to have an indicator, an operation control machine, and the keyboard and mouse as external input equipment at least. Said mouse The fingerprint which performs a discernment judging of an individual with a fingerprint detection means to detect a means to move the cursor on said drop, and the fingerprint which came to have the function to perform informational selection and cancellation / activation directions, and was formed in said mouse is detected.

[0014]

[Embodiment of the Invention] With reference to a drawing, the gestalt of the operation of a computer system using the mouse with an identification function by the fingerprint by this invention is explained below.

[0015] Drawing 1 is drawing showing the appearance configuration of the computer system using the mouse with an identification function by the fingerprint.

[0016] As shown in drawing 1, the computer system using the mouse with an identification function by the fingerprint by this invention consists of the operation control machine 1 as an operation control means, an indicator 2 as a display means, and the keyboard 3 and mouse 4 as external input equipment (external input means).

[0017] as shown in drawing 1, the operation control machine 1 as an operation control means consists of an external I/O control unit (not shown) which controls CPU (a central processing unit — not shown) which performs operation and control, the storage (memory — not shown) which memorizes a program and data, and an external I/O device.

[0018] Moreover, the indicator 2 as a display means consists of the CRT display connected to the external I/O control device of said operation control machine 1, a liquid crystal display, a plasma display, etc., and the keyboard 3 and mouse 4 as external input equipment perform the input from the outside, informational selection, cancellation, activation directions, etc.

[0019] Drawing 2 (a) is drawing which saw through the fingerprint detection equipment as a fingerprint detection means built into said mouse from the flat surface, and (b) is drawing seen through from the side face of (a).

[0020] As shown in drawing 2 (a), said mouse 4 serves as magnitude which can be grasped in the palm, and is movable free on a flat surface.

[0021] Said mouse 4 contains the positioning device 10 as a means to move the cursor on said drop 2 which consists of a CRT display, a liquid crystal display, a plasma display, etc. The positioning device 10 builds in the ball (not shown) which touches the flat surface where this mouse 4 was laid in the base of a mouse 4, it changes the rotation of this ball into a pulse, counts a pulse number, calculates the direction and relative amount of migration, and moves the cursor on said drop 2. The top face of said mouse 4 is equipped with the switch carbon button 11 which performs informational selection and cancellation / activation directions.

[0022] In addition, although said positioning device 10 by this example is considered as the configuration which uses a ball, it may be based not only on this configuration but on optical detection well-known, for example.

[0023] Moreover, as shown in drawing 2 (a), the fingerprint detection equipment 12 as a fingerprint detection means to detect a fingerprint is built in the side face a of said mouse 4.

[0024] Fingerprint detection equipment 12 consists of a CCD sensor 18 as an image pick-up means to picturize the light from the prism 17 as a reflective means of light which reflects the light from the light source 16 as a Mitsuteru gunner stage, and said light source, and said prism 17, and is contained inside the mouse 4.

[0025] In addition, other fingerprint detection means may be used for said CCD sensor 18 used for said fingerprint detection equipment 12. For example, it can replace with said CCD sensor 18, and a semi-conductor sensor can also be used. When using this semi-conductor sensor, said light source 16, prism 17, etc. can be omitted suitably. Therefore, if said semi-conductor sensor is used, the miniaturization of equipment can be attained further.

[0026] As shown in drawing 2 (a), the reflector of said prism 17 as a reflective means of light is arranged in the side face a of a mouse 4, i.e., the part which the finger (it is the thumb when operating it with the right hand) of a palm touches at the time of actuation of a mouse 4. The light source 16 as a Mitsuteru gunner stage has composition which always irradiates light to the plane of incidence of prism 17 after powering on to a computer system.

[0027] Moreover, as shown in drawing 2 (b), the impression is established in the part which the finger of the side face a of a mouse 4 touches. This is for always specifying a finger as the regular location, in order to ensure detection of the fingerprint of the finger under actuation of a mouse 4. Therefore, since the thumb is being fixed to the impression of the side face of a mouse also in migration actuation of a mouse, there is no change of the location of the thumb and it is certainly stuck to the intrados of the thumb in the reflector of prism 17.

[0028] In addition, although the example of the mouse actuation by this invention described

actuation with the right hand, actuation with the left hand is possible by arranging fingerprint detection equipment 12 so that the reflector of the prism 17 of the fingerprint detection equipment 12 of said mouse 4 may be located in the side face b of a mouse 4.

[0029] Moreover, although the fingerprint detection equipment 12 as a fingerprint detection means of said mouse 4 has the composition of detecting the fingerprint of the thumb from the side face of said mouse 4, it may prepare the reading section of the fingerprint detection equipment 12 as said fingerprint detection means in the top face of said mouse 4. In this case, although especially the finger that detects a fingerprint is not limited, since normal operation of the switch carbon button 11 which performs informational selection and cancellation / activation directions on the top face of said mouse 4 is carried out by the index finger, it should just detect the fingerprint of this index finger, for example. And it is still more suitable if the reading section and said switch carbon button 11 of fingerprint detection equipment 12 of said fingerprint detection means are made to serve a double purpose.

[0030] Below, the fingerprint detection approach in said fingerprint detection equipment 12 at the time of actuation of a mouse 4 is described.

[0031] As shown in c of drawing 2 (a), incidence of the light from the light source 16 is carried out to the plane of incidence of prism 17, it is reflected in the reflector of prism 17, and incidence of the reflected light is carried out to the CCD sensor 18.

[0032] As shown in drawing 2 (a) and (b), actuation of a mouse 4 If fixed maintenance of the thumb is carried out into the impression of the side face a of a mouse 4 and it is stuck to the intrados of the thumb in the reflector of prism 17 In the non-contact section (the crevice of a fingerprint, valley line) of the fingerprint of the intrados of the thumb, and the reflector of prism 17, the glass and air of prism 17 serve as an interface, and total reflection of the light which carried out incidence is carried out in a reflector, without leaking out of prism 17.

[0033] On the other hand, since the refractive index of the moisture of the front face of a finger differs from the refractive index of air when the heights (crest) of a fingerprint touch the reflector of prism 17, the light which carried out incidence leaks from the reflector of prism 17 outside, or is reflected irregularly in a reflector.

[0034] Therefore, the signal according to the irregularity of a fingerprint can be acquired by picturizing the reflected light from prism 17 by the CCD sensor 18. That is, the level of the output signal of the CCD sensor 18 in the crest of a fingerprint becomes low by dispersion of the light in the reflector of prism 17, and the level of the output signal of the CCD sensor 18 in the valley line of a fingerprint becomes high by the total reflection of the light in the reflector of prism 17.

[0035] The image data of said fingerprint read with fingerprint detection equipment 12 is incorporated by the interface circuitry 19 inside a mouse 4 by the storage (memory) as a storage means of the operation control machine 1 from the input/output port (for example, RS-232C, the USB port which are a serial port) of the external I/O control unit of the operation control machine 1.

[0036] said operation control machine 1 should pass the input/output port of said external I/O control device from fingerprint detection equipment 12 -- a judgment of authorization of AKUSEKU to said computer system or disapproval is made by the collating result with registration of the inputted fingerprint information (image data of a fingerprint), and collating with the fingerprint information and registered fingerprint information which carried out reading appearance for every fixed time amount from said fingerprint detection equipment 12. Moreover, the manager which performs authorization of registration of said fingerprint information, collating of fingerprint information, and access to a computer system or decision processing of disapproval is stored in the storage as a storage means of said operation control machine 1.

[0037] In addition, registration of said fingerprint information registers by the first check program after powering on to said computer system. Therefore, third parties other than the person to whom registration of this fingerprint information was given can re-register fingerprint information, or have

not changed it.

[0038] Next, processing of said operation control machine 1 about the registration means of the fingerprint information (image data of a fingerprint) read with fingerprint detection equipment 12 and the collating means of a fingerprint is explained.

[0039] The operation control machine 1 incorporates the fingerprint information (image data of a fingerprint) read with the fingerprint detection equipment 12 of a mouse 4 to an internal store, and changes [ the image data of this incorporated fingerprint ] the valley line of white information and a fingerprint into the binary-ized image of black information for the crest of a fingerprint with the threshold for binary-ized processing as a digitization means. The crest which is the white information on said binary-ized image is expressed as a line with width of face of several pixels.

[0040] Next, thinning is performed to said binary-ized image, and the crest of the fingerprint which is a line with width of face is changed into the image (thin line image) of the line of 1-pixel width of face. Thinning is pretreatment for performing easily extract processing of the focus performed to a degree.

[0041] The focus is extracted to the two-dimensional thin line image obtained by thinning using a 3 pixel (line writing direction) x3 pixel (the direction of a train) mask filter (focus extract processing).

[0042] As shown in drawing 3 (a) and (b), the focus of the thin line image of a fingerprint an endpoint (the point that a thin line breaks off, drawing 3 (a)), and the branch point (the point that a thin line branches --) It is classified into ( drawing 3 (b)), x and the y-axis which make the upper left of an image plane a home position are set up, and it is expressed with the include angle (theta) which shows the direction of the thin line extended from the location (X, Y) and the focus of each point on x and the y-axis.

[0043] Registration of a fingerprint is stored in the storage of the operation control machine 1 by using as fingerprint registration data the data of an include angle (theta) in which the direction of the thin line extended from the location (X, Y) of the focus and the focus is shown.

[0044] The collating means of a fingerprint judges the similarity of the fingerprint registration data as the focus of the fingerprint (registration fingerprint) beforehand stored in the store of the operation control machine 1, and the data of the focus of the fingerprint (input fingerprint) which was read with fingerprint detection equipment 12 and which should be collated with the operation control machine 1.

[0045] The alignment processing for doubling the coordinate of the data of the focus of the fingerprint read with said fingerprint detection equipment 12 detects the focus (it is henceforth called adjustment pair) candidate for coordinate adjustment from the data of the focus of an input fingerprint, and moves the focus of an input fingerprint to the location whose fingerprint registration data as the focus of a registration fingerprint an adjustment pair suits most.

[0046] It judges how much number of the focus which is in agreement with the fingerprint registration data as the focus of a registration fingerprint, and the data of the focus of an input fingerprint there are after processing of said alignment.

[0047] It judges by whether it is less than the allowed value to which the difference of the include angle whether it is the focus in agreement indicates the coordinate of the focus of a registration fingerprint and an input fingerprint and the direction of a thin line to be was set beforehand. It judges that the focus was in agreement when the difference of the include angle which shows the coordinate of the focus of a registration fingerprint and an input fingerprint and the direction of a thin line was less than the allowed value set up beforehand, and with an allowed value [ more than ], it is judged that the focus is not in agreement.

[0048] Below, the identification approach in the computer system by this invention is explained with reference to the flow chart shown in drawing 4 and drawing 5 .

[0049] Drawing 4 is drawing showing the flow chart about new registration of a fingerprint, a permutation, and deletion.

[0050] With reference to the flow chart shown in drawing 4 , registration and the deletion approach

of the manager a computer system's and a general user's fingerprint information are explained.

[0051] First, it is confirmed whether registration of the fingerprint of the manager of a computer system is completed (step S1). Said managers are those who manage all managements of this computer system, and are a person of the position as the so-called person in charge. Therefore, it will be the requisite that said manager operates said computer system, or said manager operates under presence the new registration of a general user mentioned later.

[0052] When said fingerprint registration is not completed, the image data of a manager's fingerprint is read in the fingerprint detection equipment 12 of said mouse 4 to the store of the operation control machine 1 (step S2). Said binary-ized processing, said thinning, and extract processing of the focus of said fingerprint are performed, and the image data of a manager's read fingerprint stores the data of the extracted focus in the storage of the operation control machine 1 as registration data of a fingerprint (step S3), and ends fingerprint registration of a manager. As already stated, it is only carrying out first, and third parties other than a manager can register a fingerprint, or registration of this manager's fingerprint can be changed no longer.

[0053] Moreover, when fingerprint registration of a manager is completed at said step S1, the fingerprint of the manager of a computer system is read in the fingerprint detection equipment 12 of said mouse 4 (step S4). Said binary-ized processing, said thinning, and extract processing of the focus of said fingerprint are performed, and the image data of the fingerprint of the manager of the read computer system performs collating with the data of the extracted focus, and the registration data of the fingerprint registered beforehand (step S5).

[0054] In addition, collating with the image data of the read fingerprint and the registration data of the fingerprint registered beforehand is performed by the fingerprint authentication means mentioned above.

[0055] As a result of collating a fingerprint, it judges whether the image data of the read fingerprint and the registration data of the fingerprint registered beforehand are in agreement (step S6). As a result of collating, when not in agreement, it judges that he is not the manager of a computer system, and processing is ended.

[0056] In said step S6, as a result of collating a fingerprint, when the image data of the read fingerprint and the registration data of the fingerprint registered beforehand are in agreement, it is regarded as the manager of a computer system and deletion of new registration of a general user's following fingerprints, permutation registration, or a registration fingerprint is performed.

[0057] Said computer system can select two or more general users with a registration manager able to use said computer system, when a registration manager's fingerprint judges it as a match in step S6. Therefore, in being [ manager / registration ] unnecessary in registration of a general user, the flow of step S7 thru/or step S9 is omitted, and shifts to the process of permutation registration of the fingerprint of step S11, and new registration of the fingerprint of step S10.

[0058] First, the fingerprint detection equipment 12 of said mouse 4 reads a general user's fingerprint (step S7), and performs collating with the data of the focus with which said binary-ized processing of the image data of the read fingerprint, said thinning and the extract processing deed of the focus of said fingerprint, and the fingerprint were extracted, and the registration data of the fingerprint registered beforehand (step S8).

[0059] In said step S8, it judges whether the collated result is in agreement with a registration fingerprint (step S9). When not in agreement with a registration fingerprint, new fingerprint registration is performed (step S10). This new fingerprint registration is new fingerprint registration of a general user, said manager will operate it or actuation under a manager's presence will be performed.

[0060] Moreover, when the collated result is in agreement, (step S11) and the following processings are performed depending on whether they are permutation registration of fingerprint data, or deletion of a registration fingerprint.

[0061] At the time of permutation registration, the registration data of the fingerprint registered into



the store of the intermediary operation control machine 1 are deleted, it stores in the store of the operation control machine 1 by using as registration data the data of the focus of the fingerprint read this time (step S12), and before replaces fingerprint data.

[0062] Said permutation registration is performed, when the already registered fingerprint is not clear and it changes the finger which performs the case where it newly transposes to a clear fingerprint, and fingerprint registration.

[0063] When it is not said permutation registration at step S11, it checks whether it is deletion of a registration fingerprint (step S13), and the registration data of the fingerprint registered are deleted at the time of deletion of a registration fingerprint (step 14).

[0064] By the above processing, new registration of the manager a computer system's and a general user's fingerprint information, permutation registration, or processing of deletion is ended.

[0065] next, a computer system explains the management tool of the fingerprint which performs authorization or the disapproval of access to a collating means to collate the fingerprint information (image data of a fingerprint) which carried out reading appearance, and registered fingerprint information (registration data of a fingerprint), and a computer system with reference to the flow chart of drawing 5.

[0066] In addition, the fingerprint registration shown with the flow chart shown in drawing 4 shall be ended.

[0067] First, said operation control machine 1 performs program execution of fingerprint management with the interrupt signal (step S21) emitted with a fixed time interval from the control manager of a computer system during application program activation. In addition, said interrupt signal may be emitted not only this but the thing by which a signal is always emitted, and at any time, although it is what is emitted with a fixed time interval.

[0068] Said operation control machine 1 reads the image data of the fingerprint from fingerprint detection equipment 12 (step S22). Said binary-ized processing (step S23), said thinning (step S24), and extract processing (step S25) of the focus of said fingerprint are performed, and, as for the image data of the fingerprint read in fingerprint detection equipment 12, the data of the focus are created. The description data of the created fingerprint perform collating with the registration data of the fingerprint with which intermediary registration even of before is carried out (step S26). In addition, collating with the image data of the read fingerprint and the registration data of the fingerprint registered beforehand is performed by the fingerprint authentication means mentioned above.

[0069] The collated result performs the following processings (step S27).

[0070] When both data are in agreement by collating with the image data of a fingerprint and the registration data of a fingerprint which were read, the program execution of fingerprint management is ended and it moves to activation of an application program (step S29). Thereby, as long as a user's fingerprint is in agreement, access to a computer system is permitted and it becomes usable [ a computer ] continuously.

[0071] By collating with the image data of a fingerprint and the registration data of a fingerprint which were read, when not in agreement, it is judged as an inaccurate user, display and unjust utilization to a control manager are notified for the message of unjust utilization (step S28), and treatment which makes access to a computer system disapproval is performed.

[0072] since access of a computer system cannot be performed if collating of the image data of a fingerprint and the registration data of a fingerprint which carried out reading appearance for every fixed time amount is performed and it is not in agreement by collating from fingerprint detection equipment 12, as stated above -- for example, -- on the way -- it can come out and \*\*\*\*\* can also prevent [ a user ] an unauthorized use. Therefore, since it is prepared in the mouse 4, if the fingerprint detection equipment 12 by this invention has the working computer system, it can always perform a user's identification.

[0073] Moreover, although the fingerprint detection equipment 12 by this invention is considered as



the configuration built in the mouse 4, you may make it equip the external side face of the keyboard 3 as external input equipment with the same configuration.

[0074] moreover -- although it excels in security also in domestic by the rapid spread of the Internet and a thing of a cheap configuration is moreover desired in recent years, if it is that by which fingerprint detection equipment 12 is built in the mouse like this invention -- anyone -- although -- connecting with a computer system easily is possible, and moreover, actuation is easy and cheap. And when accessing only specific software, you may make it apply fingerprint reading (step S7) of a general user, although it is possible to use the thing given in a flow chart shown in drawing 4 when applying the identification approach in the computer system and this computer system using the mouse with an identification function by the fingerprint by this invention to a domestic computer.

[0075] Moreover, of course, it is possible to carry out adjustable suitably and to apply within the limits of the meaning of this invention.

[0076]

[Effect of the Invention] As stated above, since the user of a computer system does not need to perform authorization procedure actuation for a computer activity by building fingerprint detection equipment in a mouse, according to this invention, it excels in convenience. Moreover, since a fingerprint is collated for every fixed time amount, when a user replaces on the way, access to a computer serves as disapproval and can form the high computer system of security.

[0077] moreover -- if according to this invention it excels in security also in domestic by the rapid spread of the Internet, and a thing of a cheap configuration is moreover desired in recent years, but it is what is built in the mouse like this invention -- anyone -- although -- connecting with a computer system easily is possible, and moreover, actuation is easy and cheap.

---

[Translation done.]

\* NOTICES \*

JPO and NCIP are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the appearance configuration of the computer system using the mouse with an identification function by the fingerprint.

[Drawing 2] Drawing which saw through the fingerprint detection equipment as that of a fingerprint detection means by which (a) was included in the mouse, from the flat surface, and (b) are drawings seen through from the side face of the mouse shown in (a).

[Drawing 3] It is drawing showing the focus of a fingerprint image, and (a) shows an endpoint and (b) shows the branch point.

[Drawing 4] It is a flow chart about new registration of a fingerprint, a permutation, and deletion.

[Drawing 5] It is the flow chart which shows the collating means of a fingerprint, and the management tool of a fingerprint.

[Description of Notations]

- 1 Operation Control Machine
- 2 Drop
- 3 Keyboard
- 4 Mouse
- 10 Positioning Device
- 11 Switch Carbon Button
- 12 Fingerprint Detection Equipment
- 16 Light Source
- 17 Prism
- 18 CCD Sensor
- 19 Interface Circuitry

---

[Translation done.]

\* NOTICES \*

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

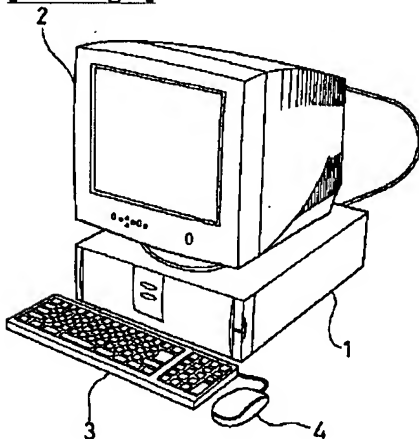
2.\*\*\*\* shows the word which can not be translated.

3.In the drawings, any words are not translated.

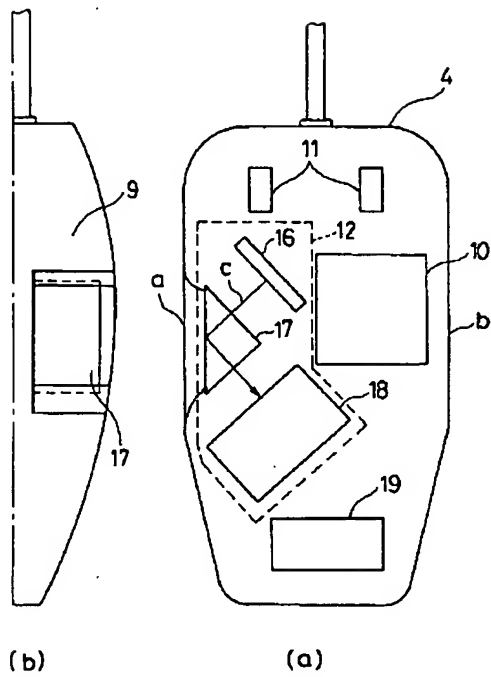
---

DRAWINGS

[Drawing 1]

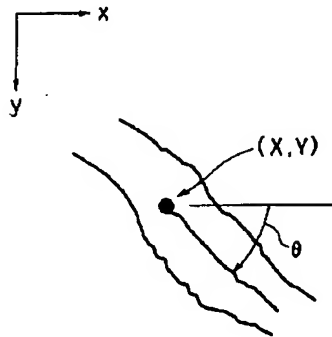


[Drawing 2]

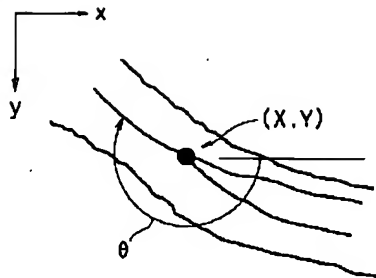


[Drawing 3]

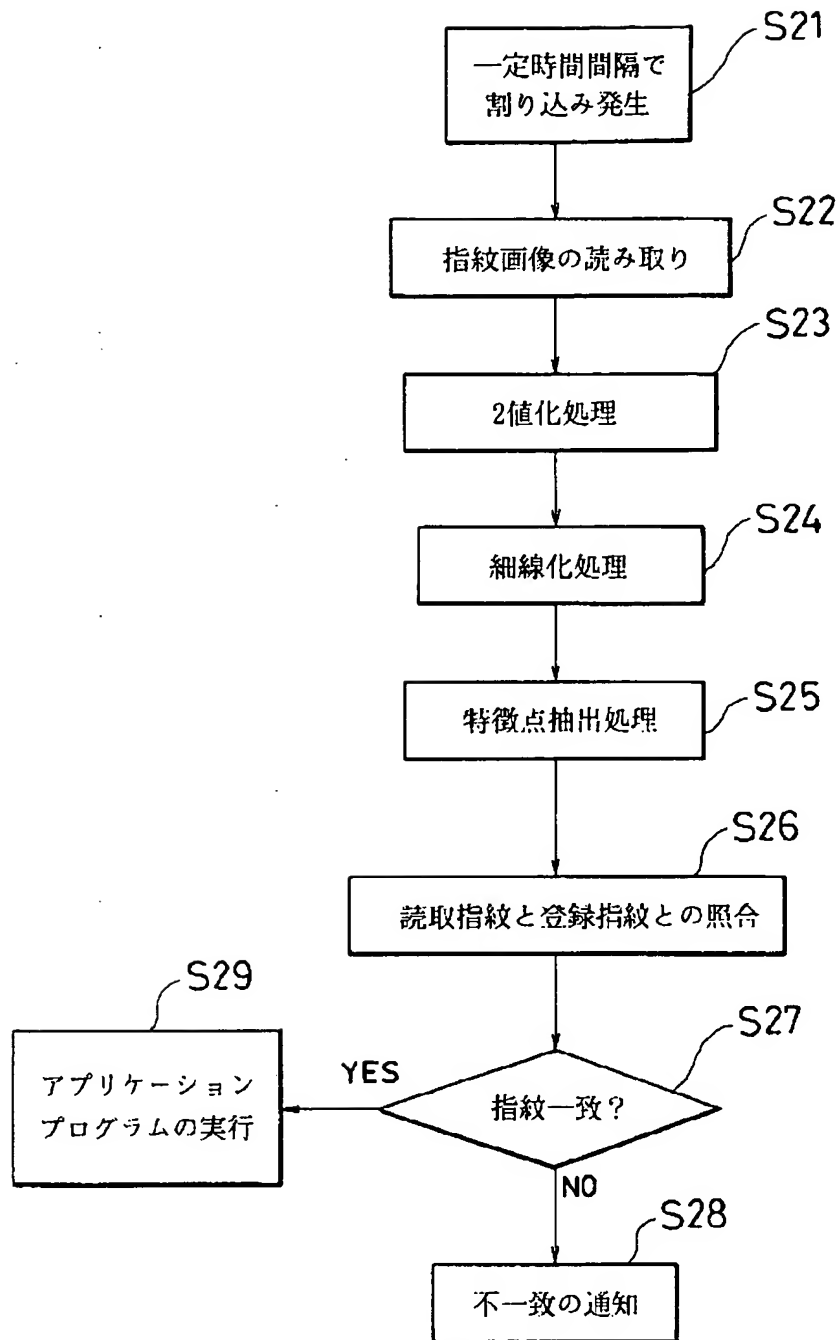
(a)



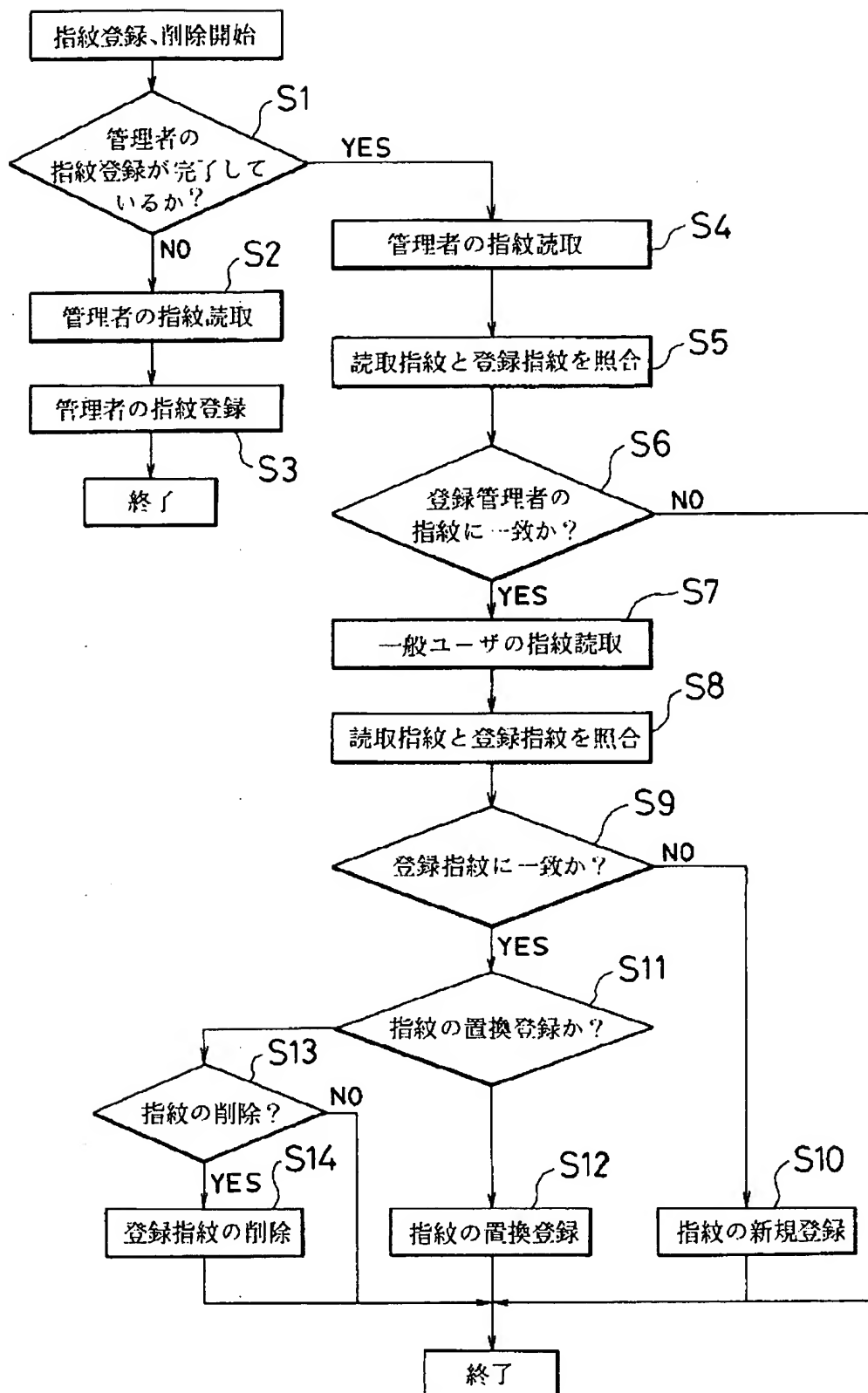
(b)



[Drawing 5]



[Drawing 4]



[Translation done.]

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-222123

(43)Date of publication of application : 11.08.2000

(51)Int.Cl.

G06F 3/033

G06F 1/00

G06F 15/00

G06T 7/00

G06T 1/00

(21)Application number : 11-027117

(71)Applicant : KOKYO JOHO SYSTEM:KK

(22)Date of filing : 04.02.1999

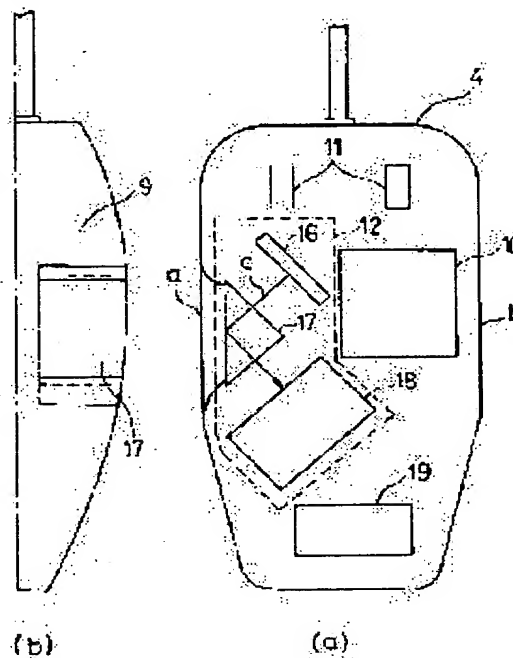
(72)Inventor : ABE MASAYOSHI  
SAKAMOTO NORINOBU

(54) COMPUTER SYSTEM USING MOUSE WITH INDIVIDUAL IDENTIFICATION FUNCTION BY FINGERPRINT AND INDIVIDUAL IDENTIFICATION METHOD IN COMPUTER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the computer system of high security capable of surely checking the unauthorized utilization of the computer system.

SOLUTION: A fingerprint detector 12 for detecting fingerprints is incorporated in a mouse 4, a means for registering fingerprint information inputted from the fingerprint detector 12 is arranged and an individual is identified by collating the fingerprint information read at every constant interval of time from the fingerprint detector 12 and already registered fingerprint information by a collation means. By the collated result of the collation means, the permission or denial of access to this computer system is judged.



## LEGAL STATUS

[Date of request for examination]

04.02.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3224216

[Date of registration]

24.08.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

24.08.2004

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-222123

(P2000-222123A)

(43) 公開日 平成12年8月11日 (2000.8.11)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 3/033	3 4 0	G 0 6 F 3/033	3 4 0 C 5 B 0 4 3
1/00	3 7 0	1/00	3 7 0 E 5 B 0 4 7
15/00	3 3 0	15/00	3 3 0 F 5 B 0 8 5
G 0 6 T 7/00		15/62	4 6 0 5 B 0 8 7
1/00		15/64	G
審査請求 有 請求項の数 5 O L (全 10 頁)			

(21) 出願番号 特願平11-27117

(22) 出願日 平成11年2月4日 (1999.2.4)

(71) 出願人 599016523

公共情報システム株式会社

東京都中央区東日本橋2丁目15番5号

(72) 発明者 阿部 正良

東京都中央区東日本橋2丁目15番5号 公  
共情報システム株式会社内

(72) 発明者 坂本 典信

東京都中央区東日本橋2丁目15番5号 公  
共情報システム株式会社内

(74) 代理人 100081318

弁理士 羽切 正治

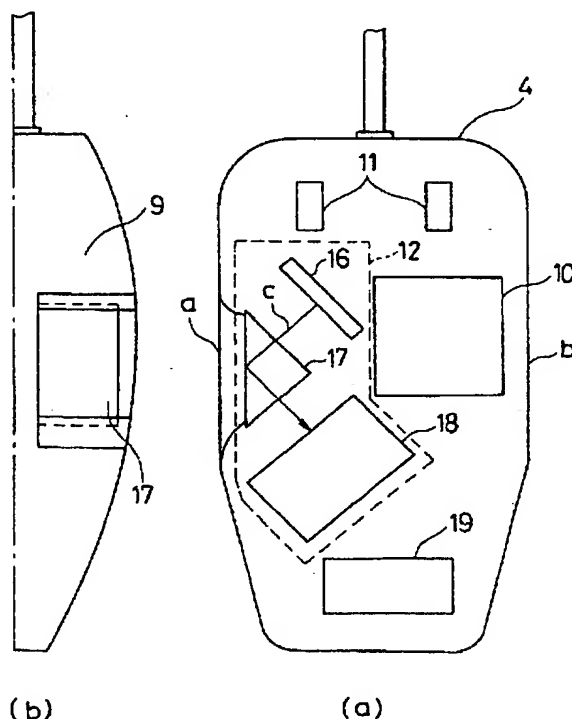
最終頁に続く

(54) 【発明の名称】 指紋による個人識別機能付きマウスを用いたコンピュータシステム及び該コンピュータシステムにおける個人識別方法

(57) 【要約】

【課題】 コンピュータシステムの不正利用を確実にチェックすることが可能なセキュリティの高いコンピュータシステムを提供すること。

【解決手段】 指紋を検出する指紋検出装置12をマウス4に内蔵し、前記指紋検出装置12から入力された指紋情報を登録する手段と、前記指紋検出装置12から一定時間毎に読み出した指紋情報と登録済み指紋情報とを照合手段により照合して個人識別を行い、前記照合手段の照合結果により前記コンピュータシステムへのアクセスの許可又は不許可の判断を行う。





**【特許請求の範囲】**

【請求項1】 少なくとも、表示器と、演算制御機と、外部入力装置としてのキーボード及びマウスとを備えるコンピュータシステムであって、

前記マウスは、前記表示器上のカーソルを移動する手段と、情報の選択・取消・実行指示を行う機能を備えるとともに、前記マウスに指紋を検出する指紋検出手段を前記マウスに設けたことを特徴とする指紋による個人識別機能付きマウスを用いたコンピュータシステム。

【請求項2】 前記指紋検出手段は、光照射手段としての光源と、前記光源からの光を反射する光の反射手段としてのプリズムと、前記プリズムからの光を撮像する撮像手段としてのCCDセンサよりなることを特徴とする請求項1記載の指紋による個人識別機能付きマウスを用いたコンピュータシステム。

【請求項3】 前記指紋検出手段は、半導体センサであることを特徴とする請求項1記載の指紋による個人識別機能付きマウスを用いたコンピュータシステム。

【請求項4】 前記演算制御機は、前記指紋検出手段から入力された指紋情報を登録する登録手段と、前記指紋検出手段から一定時間毎に読み出した指紋情報と登録済み指紋情報とを照合する照合手段と、前記照合手段の照合結果により前記コンピュータシステムへのアクセスの許可又は不許可の判断を行う指紋の管理手段を備えてなることを特徴とする請求項1記載の指紋による個人識別機能付きマウスを用いたコンピュータシステム。

【請求項5】 少なくとも、表示器と、演算制御機と、外部入力装置としてのキーボード及びマウスとを備えるコンピュータシステムを用いた個人識別方法であって、

前記マウスは、前記表示器上のカーソルを移動する手段と、情報の選択・取消・実行指示を行う機能を備えてなり、前記マウスに設けられた指紋を検出する指紋検出手段により個人の識別判定を行う指紋を検出することを特徴とするコンピュータシステムにおける個人識別方法。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】 本発明は、指紋検出手段を備えたマウスによる個人の識別に関するセキュリティ機能の向上を図り、しかも前記マウスによる個人の識別管理をコンピュータシステムの稼働状態中に自動的に行うことが可能な指紋による個人識別機能付きマウスを用いたコンピュータシステム及び該コンピュータシステムにおける個人識別方法に関する。

**【0002】**

【従来の技術】 近年、コンピュータシステムは、インターネット、企業内ネットワーク等の普及に伴って複数の利用者の特定のためにパスワードの使用が図られている。パスワードが一致することによりインターネットへの接続やネットワークへの接続、並びにコンピュータシ

ステムの使用、データベースへのアクセス等の許可又は不許可が図られている。

【0003】 このようなパスワードの利用は、利用者の特定が容易にできるという利便性がある反面、前記パスワードは一回入れれば足りるためコンピュータシステムが稼働中であれば前記パスワードを知らない第三者であっても前記システムの内部に容易にアクセスすることが可能である。また、前記パスワードが他人に知られて不正に使用されると前記コンピュータシステムを電源投入時から簡単に不正利用することが可能となり、コンピュータシステムのセキュリティ機能の向上を図る上でも改善すべき課題となっている。

【0004】 このようなセキュリティの改善を図る手段として、パスワードではなく、利用者の個人毎の指紋を登録しておき、コンピュータシステムの使用時に別の装置である指紋読み取り専用装置を別途用意して指紋照合の手続を行った上でコンピュータシステムへのアクセスの許可又は不許可を判定してコンピュータシステムのセキュリティ機能の向上を確保することが行われている。

**【0005】**

【発明が解決しようとする課題】 前述したパスワードによる利用者の確認は、通常数字や文字、記号の組み合わせ等からなるものであるため、比較的解読されやすく、一度解読されてしまうと、パスワードの変更を行うまでは自由にアクセスが可能になってしまうという問題があり、また、指紋の照合による利用者の確認は、指紋が個人毎に異なるためセキュリティの面からは向上するものの前記コンピュータシステムの指紋を読み取るための専用装置である指紋読取装置が別途必要となり、ダウンサイジングが図られつつある今日において省スペース化が困難となり、しかも高価なものになってしまうという課題がある。しかも、この指紋読取装置は指紋の照合を行う毎に、別途指紋照合手続が必要となり利便性に欠けている。また、前記指紋読取装置は、指紋照合手続で一度照合にパスすると、以後指紋の照合無しでコンピュータシステムの利用ができるため、途中で利用者が替わってもチェックされず不正に使用される恐れがあり、コンピュータシステムのセキュリティ上改善すべき課題となっている。

【0006】 そこで本発明は、前記従来の技術に鑑みて成されたものであって、個人の同定、すなわち個人の判別又は識別方法として確立している指紋を利用してコンピュータシステムのセキュリティ機能の向上を図るものである。すなわち、指紋検出手段を外入力装置であるマウスに設けることにより、一定時間毎に前記マウスの指紋検出手段から指紋の画像を読み取り、この読み取った指紋データと登録された指紋データとの照合を行い、利用者の同定を行うことが可能な指紋による個人識別機能付きマウスを用いたコンピュータシステム及び該コンピュータシステムにおける個人識別方法を提供すること

を目的とするものである。

【0007】また、指紋検出手段をマウスに設けたことにより利用者は専用装置としての指紋読取装置で別途指紋照合手続を行う必要がなく、利便性に優れた指紋による個人識別機能付きマウスを用いたコンピュータシステム及び該コンピュータシステムにおける個人識別方法を提供することを目的とするものである。

【0008】また、近年、インターネットの急速な普及により家庭内においてもセキュリティに優れたしかも安価な構成のものが望まれており、かかる面からみても好適な指紋による個人識別機能付きマウスを用いたコンピュータシステム及び該コンピュータシステムにおける個人識別方法を提供することを目的とするものである。

【0009】

【課題を解決するための手段】本発明による指紋による個人識別機能付きマウスを用いたコンピュータシステムは、少なくとも、表示器と、演算制御機と、外部入力装置としてのキーボード及びマウスとを備えてなるコンピュータシステムであって、前記マウスは、前記表示器上のカーソルを移動する手段と、情報の選択・取消・実行指示を行う機能を備えるとともに、前記マウスに指紋を検出する指紋検出手段を前記マウスに設けたものである。

【0010】また、本発明による指紋による個人識別機能付きマウスを用いたコンピュータシステムの前記指紋検出手段は、光照射手段としての光源と、前記光源からの光を反射する光の反射手段としてのプリズムと、前記プリズムからの光を撮像する撮像手段としてのCCDセンサよりなるものである。

【0011】また、本発明による指紋による個人識別機能付きマウスを用いたコンピュータシステムの前記指紋検出手段は、半導体センサでなるものである。

【0012】また、本発明による指紋による個人識別機能付きマウスを用いたコンピュータシステムの前記演算制御機は、前記指紋検出手段から入力された指紋情報を登録する登録手段と、前記指紋検出手段から一定時間毎に読み出した指紋情報と登録済み指紋情報とを照合する照合手段と、前記照合手段の照合結果により前記コンピュータシステムへのアクセスの許可又は不許可の判断を行う指紋の管理手段を備えてなるものである。

【0013】また、本発明によるコンピュータシステムにおける個人識別方法は、少なくとも、表示器と、演算制御機と、外部入力装置としてのキーボード及びマウスとを備えてなるコンピュータシステムを用いた個人識別方法であって、前記マウスは、前記表示器上のカーソルを移動する手段と、情報の選択・取消・実行指示を行う機能を備えてなり、前記マウスに設けられた指紋を検出する指紋検出手段により個人の識別判定を行う指紋を検出するものである。

【0014】

【発明の実施の形態】以下図面を参照して、本発明による指紋による個人識別機能付きマウスを用いたコンピュータシステムの実施の形態について説明する。

【0015】図1は、指紋による個人識別機能付きマウスを用いたコンピュータシステムの外観構成を示す図である。

【0016】図1に示すように、本発明による指紋による個人識別機能付きマウスを用いたコンピュータシステムは、演算制御手段としての演算制御機1と、表示手段としての表示器2と、外部入力装置（外部入力手段）としてのキーボード3及びマウス4とからなっている。

【0017】図1に示すように、演算制御手段としての演算制御機1は、演算、制御を行うCPU（中央演算装置、図示せず）と、プログラム、データを記憶する記憶装置（メモリ、図示せず）と、外部の入出力装置の制御を行う外部入出力制御装置（図示せず）からなる。

【0018】また、表示手段としての表示器2は、前記演算制御機1の外部入出力制御装置に接続されたCRTディスプレイ、液晶ディスプレイ、プラズマディスプレイ等からなり、外部入力装置としてのキーボード3及びマウス4は、外部からの入力、情報の選択、取消、実行指示等を行うものである。

【0019】図2（a）は、前記マウスに組み込まれた指紋検出手段としての指紋検出装置を平面から透視した図であり、（b）は、（a）の側面から透視した図である。

【0020】図2（a）に示すように、前記マウス4は、手のひらで握れる大きさとなっており、平面上で自在に移動可能となっている。

【0021】前記マウス4は、CRTディスプレイ、液晶ディスプレイ、プラズマディスプレイ等からなる前記表示器2上のカーソルを移動する手段としての位置決め機構10を内蔵している。位置決め機構10は、マウス4の底面に該マウス4が載置された平面と接するボール（図示せず）を内蔵し、このボールの回転量をパルスに変換してパルス数をカウントして移動の方向と相対量を求め、前記表示器2上のカーソルを移動する。前記マウス4の上面には、情報の選択・取消・実行指示を行うスイッチボタン11が備えられている。

【0022】なお、本実施例による前記位置決め機構10は、ボールを用いる構成としているが、この構成に限らず、例えば公知の光学的な検出によるものでもよい。

【0023】また、図2（a）に示すように、前記マウス4の側面aには、指紋を検出する指紋検出手段としての指紋検出装置12が内蔵されている。

【0024】指紋検出装置12は、光照射手段としての光源16、前記光源からの光を反射する光の反射手段としてのプリズム17、前記プリズム17からの光を撮像する撮像手段としてのCCDセンサ18からなり、マウス4の内部に収納されている。

【0025】なお、前記指紋検出装置12に使用される前記CCDセンサ18は、他の指紋検出手段を使用するものでもよい。例えば、前記CCDセンサ18に代えて半導体センサを使用することもできる。この半導体センサを使用する場合には、前記光源16、プリズム17などを適宜省略することができる。従って、前記半導体センサを使用すれば、更に装置の小型化を図ることができる。

【0026】図2(a)に示すように、光の反射手段としての前記プリズム17の反射面はマウス4の側面a、すなわち、マウス4の操作時に手のひらの指(右手で操作するときには親指)が触れる個所に配設されている。光照射手段としての光源16は、コンピュータシステムへの電源投入後、常時プリズム17の入射面に対し光を照射する構成となっている。

【0027】また、マウス4の側面aの指が触れる箇所には、図2(b)に示すように、くぼみが設けられている。これはマウス4の操作中の指の指紋の検出を確実に行うために指を常に決まった位置に特定するためのものである。従って、マウスの移動操作中でも親指がマウスの側面のくぼみに固定されているため、親指の位置の変化がなく、親指の腹面がプリズム17の反射面に確実に密着される。

【0028】なお、本発明でのマウス操作の実施例は、右手での操作について述べたが、左手での操作は、前記マウス4の指紋検出装置12のプリズム17の反射面がマウス4の側面bに位置するように指紋検出装置12を配置することにより可能である。

【0029】また、前記マウス4の指紋検出手段としての指紋検出装置12は、前記マウス4の側面から親指の指紋を検出する構成となっているが、前記マウス4の上面に前記指紋検出手段としての指紋検出装置12の読み取り部を設けてもよい。この場合、指紋を検出する指は特に限定されるものではないが、例えば、前記マウス4の上面で情報の選択・取消・実行指示を行うスイッチボタン11は、人差し指で通常操作するのでこの人差し指の指紋を検出するようにすればよい。そして、前記指紋検出手段の指紋検出装置12の読み取り部と前記スイッチボタン11とを兼用すれば更に好適なものである。

【0030】以下に、マウス4の操作時の前記指紋検出装置12での指紋検出方法について述べる。

【0031】図2(a)のcに示すように、光源16からの光はプリズム17の入射面に入射してプリズム17の反射面で反射し、反射した光はCCDセンサ18に入射する。

【0032】図2(a)及び(b)に示すように、マウス4の操作は、親指がマウス4の側面aのくぼみ内に固定保持されて親指の腹面がプリズム17の反射面に密着されると、親指の腹面の指紋とプリズム17の反射面との非接触部(指紋の凹部、谷線)では、プリズム17の

ガラスと空気とが境界面となり、入射した光はプリズム17の外に漏れることなく反射面で全反射する。

【0033】他方、指紋の凸部(隆線)がプリズム17の反射面に接触しているときには、指の表面の水分の屈折率が空気の屈折率と異なるため、入射した光はプリズム17の反射面から外に漏れたり、反射面で乱反射したりする。

【0034】従って、プリズム17からの反射光をCCDセンサ18で撮像することにより、指紋の凹凸に応じた信号を得ることができる。すなわち、指紋の隆線でのCCDセンサ18の出力信号のレベルは、プリズム17の反射面での光の散乱によって低くなり、指紋の谷線でのCCDセンサ18の出力信号のレベルは、プリズム17の反射面での光の全反射によって高くなる。

【0035】指紋検出装置12で読み取った前記指紋の画像データは、マウス4の内部のインターフェース回路19により演算制御機1の外部入出力制御装置の入出力ポート(例えば、シリアルポートであるRS-232C、USBポート)より演算制御機1の記憶手段としての記憶装置(メモリ)に取り込まれる。

【0036】前記演算制御機1は、指紋検出装置12から前記外部入出力制御装置の入出力ポートを経て入力された指紋情報(指紋の画像データ)の登録と、前記指紋検出装置12から一定時間毎に読み出した指紋情報と登録済み指紋情報との照合と、照合結果により前記コンピュータシステムへのアクセスの許可又は不許可の判断を行う。また、前記演算制御機1の記憶手段としての記憶装置には、前記指紋情報の登録、指紋情報の照合、コンピュータシステムへのアクセスの許可又は不許可の判断処理を行う管理プログラムが格納されている。

【0037】なお、前記指紋情報の登録は、前記コンピュータシステムへの電源投入後、最初の確認プログラムで登録を行う。従って、この指紋情報の登録が行われた人以外の第三者は、指紋情報を再登録したり、変更したりすることができないものとなっている。

【0038】次に、指紋検出装置12で読み取った指紋情報(指紋の画像データ)の登録手段及び指紋の照合手段についての前記演算制御機1の処理を説明する。

【0039】演算制御機1は、マウス4の指紋検出装置12で読み取った指紋情報(指紋の画像データ)を内部の記憶装置に取り込み、この取り込まれた指紋の画像データをデジタル化手段としての2値化処理用のしきい値により指紋の隆線を白情報、指紋の谷線を黒情報の2値化画像に変換する。前記2値化画像の白情報である隆線は、数画素の幅を持った線として表される。

【0040】次に、前記2値化画像に対して細線化処理を行い、幅を持った線である指紋の隆線を1画素幅の線の画像(細線画像)に変換する。細線化処理は、次に行う特徴点の抽出処理を容易に行うための前処理である。

【0041】細線化処理により得られた2次元の細線画

像に対して、3画素（行方向）×3画素（列方向）のマスクフィルターを用いて特徴点の抽出を行う（特徴点抽出処理）。

【0042】図3（a）及び（b）に示すように、指紋の細線画像の特徴点は、端点（細線が途切れる点、図3（a））及び分岐点（細線が枝分かれする点、図3（b））に分類され、画像平面の左上を原点位置とするx、y軸を設定し、x、y軸上のそれぞれの点の位置（X、Y）及び特徴点から伸びる細線の方法を示す角度（ $\theta$ ）で表される。

【0043】指紋の登録は、特徴点の位置（X、Y）及び特徴点から伸びる細線の方法を示す角度（ $\theta$ ）のデータを指紋登録データとして演算制御機1の記憶装置に格納する。

【0044】指紋の照合手段は、前もって演算制御機1の記憶装置に格納されている指紋（登録指紋）の特徴点としての指紋登録データと、指紋検出装置12で読み取った照合すべき指紋（入力指紋）の特徴点のデータの類似度を演算制御機1で判定する。

【0045】前記指紋検出装置12で読み取った指紋の特徴点のデータの座標を合わせるための位置合わせ処理は、入力指紋の特徴点のデータから座標整合用の特徴点（以後、整合対と言う）候補を検出し、整合対が登録指紋の特徴点としての指紋登録データと最も合う位置に入力指紋の特徴点を移動させる。

【0046】前記位置合わせの処理後、登録指紋の特徴点としての指紋登録データと、入力指紋の特徴点のデータとで一致する特徴点の数がどの程度あるのかを判断する。

【0047】一致する特徴点か否かは、登録指紋と入力指紋の特徴点の座標及び細線の方法を示す角度の差が前もって設定された許容値以内であるかどうかで判断する。登録指紋と入力指紋の特徴点の座標及び細線の方法を示す角度の差が前もって設定された許容値以内であれば、特徴点は一致したと判断し、許容値以上であれば特徴点は一致していないと判断する。

【0048】以下に、本発明によるコンピュータシステムにおける個人識別方法について図4及び図5に示すフローチャートを参照して説明する。

【0049】図4は、指紋の新規登録、置換及び削除についてのフローチャートを示す図である。

【0050】図4に示す、フローチャートを参照して、コンピュータシステムの管理者及び一般ユーザの指紋情報の登録及び削除方法について説明する。

【0051】まず、コンピュータシステムの管理者の指紋の登録が完了しているかをチェックする（ステップS1）。前記管理者は、このコンピュータシステムの全ての管理を司る者であり、いわゆる責任者としての立場の者である。従って、後述する一般ユーザの新規登録などは、前記管理者が前記コンピュータシステムを操作する

か若しくは前記管理者が立ち会いのもとで操作することが前提となる。

【0052】前記指紋登録が完了していない場合には、前記マウス4の指紋検出装置12から演算制御機1の記憶装置に管理者の指紋の画像データを読み取る（ステップS2）。読み取られた管理者の指紋の画像データは、前記2値化処理、前記細線化処理及び前記指紋の特徴点の抽出処理が行われ、抽出した特徴点のデータを指紋の登録データとして演算制御機1の記憶装置に格納して（ステップS3）、管理者の指紋登録を終了する。この管理者の指紋の登録は、既に述べたように、最初に行うのみであり、管理者以外の第三者が指紋を登録したり、変更したりすることができないようになっている。

【0053】また、前記ステップS1で管理者の指紋登録が完了している場合には、前記マウス4の指紋検出装置12からコンピュータシステムの管理者の指紋を読み取る（ステップS4）。読み取られたコンピュータシステムの管理者の指紋の画像データは、前記2値化処理、前記細線化処理及び前記指紋の特徴点の抽出処理が行われ、抽出された特徴点のデータと前もって登録されている指紋の登録データとの照合を行う（ステップS5）。

【0054】なお、読み取られた指紋の画像データと、前もって登録されている指紋の登録データとの照合は、前述した指紋照合手段によって行われる。

【0055】指紋の照合を行った結果、読み取られた指紋の画像データと、前もって登録されている指紋の登録データが一致しているか否かを判断する（ステップS6）。照合した結果、一致していないときには、コンピュータシステムの管理者ではないと判断し、処理を終了する。

【0056】前記ステップS6において、指紋の照合を行った結果、読み取られた指紋の画像データと、前もって登録されている指紋の登録データが一致したときには、コンピュータシステムの管理者とみなし、以下の、一般ユーザの指紋の新規登録、置換登録又は登録指紋の削除を行う。

【0057】前記コンピュータシステムは、登録管理者の指紋がステップS6において一致するものと判断した場合には、登録管理者が前記コンピュータシステムを利用することが可能な一般ユーザを複数選定することができるようになっている。従って、登録管理者が一般ユーザの登録が必要ない場合にはステップS7乃至ステップS9のフローは省略され、ステップS11の指紋の置換登録、ステップS10の指紋の新規登録の工程に移行する。

【0058】まず、前記マウス4の指紋検出装置12は、一般ユーザの指紋を読み取り（ステップS7）、読み取った指紋の画像データの前記2値化処理、前記細線化処理及び前記指紋の特徴点の抽出処理を行い、指紋の抽出された特徴点のデータと、前もって登録されている指

紋の登録データとの照合を行う(ステップS8)。

【0059】前記ステップS8において、照合した結果が登録指紋と一致しているか否かを判断する(ステップS9)。登録指紋と一致しないときには、新規指紋登録を行う(ステップS10)。この新規指紋登録は、一般ユーザの新規指紋登録であって、前記管理者が操作するか若しくは管理者の立ち会いのもとでの操作が行われることとなる。

【0060】また、照合した結果が一致したときには、指紋データの置換登録又は登録指紋の削除かにより(ステップS11)、以下の処理を行う。

【0061】置換登録のときには、前もって演算制御機1の記憶装置に登録されている指紋の登録データを削除し、今回読み取った指紋の特徴点のデータを登録データとして演算制御機1の記憶装置に格納し(ステップS12)、指紋データの置き換えを行う。

【0062】前記置換登録は、既に登録されている指紋が鮮明でないときに鮮明な指紋に新たに置き換える場合や指紋登録を行う指を変える場合などに行うものである。

【0063】ステップS11で前記置換登録でないときには登録指紋の削除を確認し(ステップS13)、登録指紋の削除のときは、登録されている指紋の登録データを削除する(ステップS14)。

【0064】以上の処理で、コンピュータシステムの管理者及び一般ユーザの指紋情報の新規登録、置換登録又は削除の処理は終了する。

【0065】次に、コンピュータシステムで読み出した指紋情報(指紋の画像データ)と登録済み指紋情報(指紋の登録データ)とを照合する照合手段及び、コンピュータシステムへのアクセスの許可又は不許可を行う指紋の管理手段について図5のフローチャートを参照して説明する。

【0066】なお、図4に示すフローチャートで示した指紋登録は、終了しているものとする。

【0067】まず、アプリケーションプログラム実行中に、コンピュータシステムの制御管理プログラムから一定時間間隔で発せられる割り込み信号(ステップS21)により、前記演算制御機1は指紋管理のプログラムの実行を行う。なお、前記割り込み信号は、一定時間間隔で発せられるものとなっているが、これに限らず常時信号が発せられるものや随時発せられるものであってもよい。

【0068】前記演算制御機1は、指紋検出装置12からの指紋の画像データを読み取る(ステップS22)。指紋検出装置12から読み取られた指紋の画像データは、前記2値化処理(ステップS23)、前記細線化処理(ステップS24)及び前記指紋の特徴点の抽出処理(ステップS25)が行われ、特徴点のデータが作成される。作成された指紋の特徴データは、前もって登録さ

れている指紋の登録データとの照合を行う(ステップS26)。なお、読み取られた指紋の画像データと、前もって登録されている指紋の登録データとの照合は、前述した指紋照合手段によって行われる。

【0069】照合した結果により以下の処理を行う(ステップS27)。

【0070】読み取った指紋の画像データと指紋の登録データとの照合で両データが一致したときには、指紋管理のプログラムの実行を終了し、アプリケーションプログラムの実行に移る(ステップS29)。これにより、利用者の指紋が一致する限りコンピュータシステムへのアクセスが許可され、継続してコンピュータの使用が可能となる。

【0071】読み取った指紋の画像データと指紋の登録データとの照合で、一致しなかったときには、不正利用者と判断し、不正利用のメッセージを表示及び制御管理プログラムへの不正利用の通知を行い(ステップS28)、コンピュータシステムへのアクセスを不許可とする処置が行われる。

【0072】以上述べたように、指紋検出装置12より一定時間毎に読み出した指紋の画像データと指紋の登録データの照合が行われ、照合で一致しなければコンピュータシステムのアクセスは行えないため、例えば、途中で使用者が替わっても不正使用を防ぐことができる。従って、本発明による指紋検出装置12は、マウス4に設けられているため、コンピュータシステムが動作中であれば常に利用者の個人識別を行うことが可能である。

【0073】また、本発明による指紋検出装置12は、マウス4に内蔵されている構成としたものであるが、外部入力装置としてのキーボード3の外部側面に同一の構成を備えるようにしてもよい。

【0074】また、近年、インターネットの急速な普及により家庭内においてもセキュリティに優れしかも安価な構成のものが望まれているが、本発明のようにマウスに指紋検出装置12が内蔵されているものであれば誰でも容易にコンピュータシステムに接続することが可能であり、しかも操作が簡単で安価である。そして、本発明による指紋による個人識別機能付きマウスを用いたコンピュータシステム及び該コンピュータシステムにおける個人識別方法を家庭内のコンピュータに適用する場合には、図4に示す、フローチャート記載のものを用いることが可能であるが、特定のソフトウェアのみにアクセスする場合に一般ユーザの指紋読取(ステップS7)を適用するようにしてもよい。

【0075】また、本発明の趣旨の範囲内で適宜可変して適用することが可能であることは勿論である。

【0076】

【発明の効果】以上述べたように、本発明によれば、指紋検出装置をマウスに内蔵することにより、コンピュータシステムの利用者は、コンピュータ使用のための許可

手続き操作を行う必要がないため、利便性に優れている。また、指紋の照合を一定時間毎に行うため、途中で利用者が替わった時には、コンピュータへのアクセスが不許可となり、セキュリティの高いコンピュータシステムを形成することができる。

【0077】また、本発明によれば、近年、インターネットの急速な普及により家庭内においてもセキュリティに優れしかも安価な構成のものが望まれているが、本発明のようにマウスに内蔵されているものであれば誰でもが容易にコンピュータシステムに接続することが可能であり、しかも操作が簡単で安価である。

#### 【図面の簡単な説明】

【図1】指紋による個人識別機能付きマウスを用いたコンピュータシステムの外観構成を示す図である。

【図2】(a)はマウスに組み込まれた指紋検出手段としての指紋検出装置を平面から透視した図、(b)は(a)に示すマウスの側面から透視した図である。

【図3】指紋画像の特徴点を示す図であり、(a)は端

点、(b)は分岐点を示す。

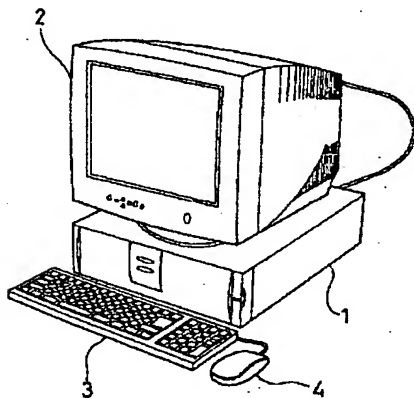
【図4】指紋の新規登録、置換及び削除についてのフローチャートである。

【図5】指紋の照合手段及び指紋の管理手段を示すフローチャートである。

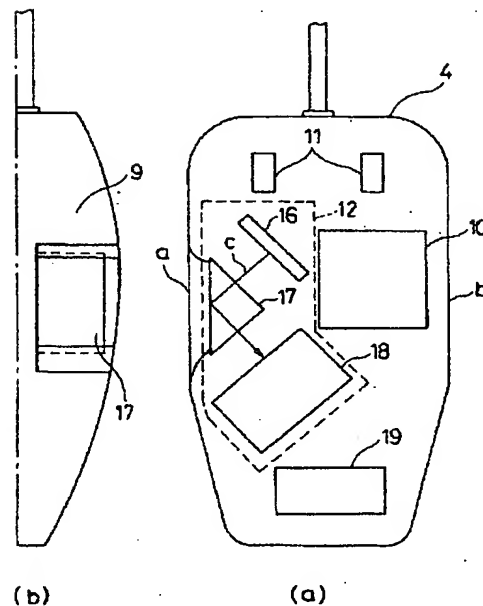
#### 【符号の説明】

- 1 演算制御機
- 2 表示器
- 3 キーボード
- 4 マウス
- 10 位置決め機構
- 11 スイッチボタン
- 12 指紋検出装置
- 16 光源
- 17 プリズム
- 18 CCDセンサ
- 19 インターフェース回路

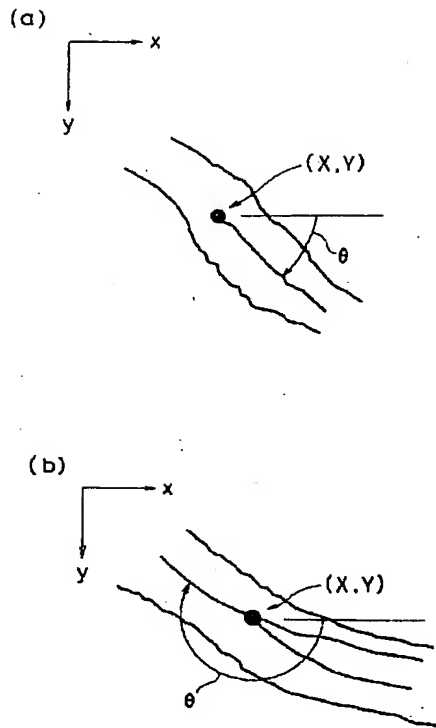
【図1】



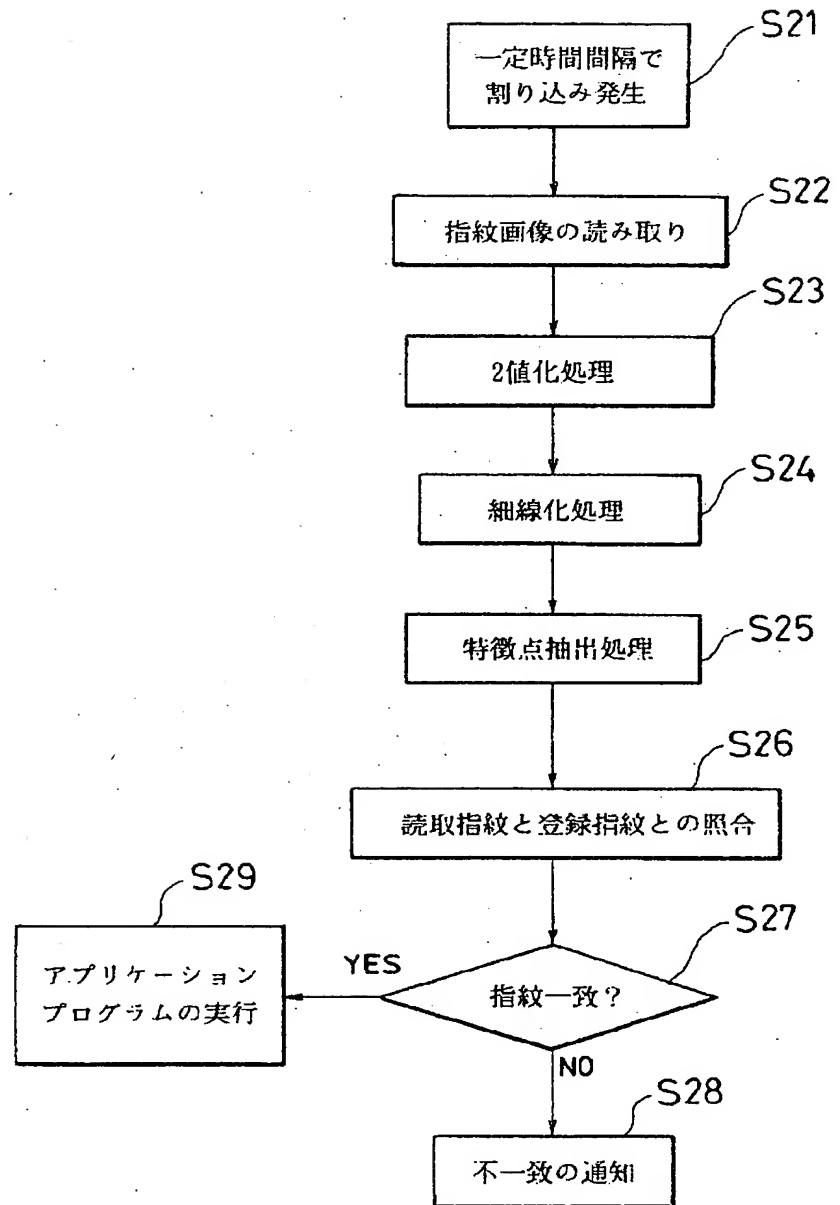
【図2】



【図3】

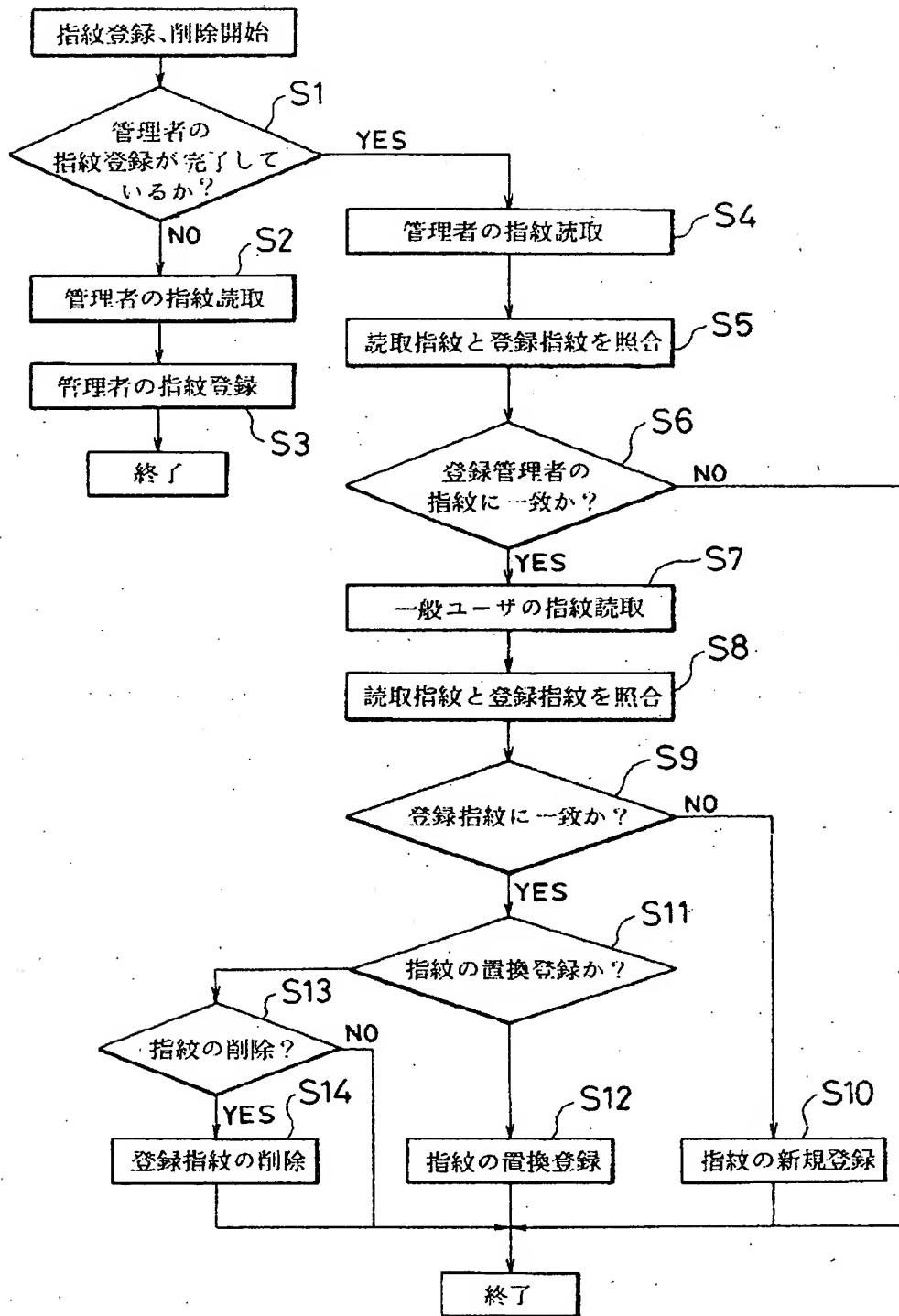


【図5】





【図4】



フロントページの続き

Fターム(参考) 5B043 AA09 BA02 DA05 FA03 GA01  
5B047 AA25 BA03 BB01 BC30  
5B085 AE26 CC02  
5B087 AA00 BB12